

IN THE CLAIMS

Please amend the claims as follows:

1. (Previously Presented) A method comprising:

performing, in a first service access provider, operations including,

receiving an access request from a client access device, the access request requesting access to a network, wherein a user associated with the client access device is a subscriber of a second service access provider;

establishing a communications link with the client access device to authenticate and authorize the user;

receiving client device configuration data from the client access device over the communications link during an authentication and authorization exchange;

transmitting the client device configuration data destined for the second service access provider, wherein the second service access provider is operable to process the client device configuration data and selectively grant the client access device access to the network based upon the client device configuration data; and

receiving an indication about whether the client access device is granted access to the network, the indication originating from the second service access provider.

2. (Original) The method of claim 1, wherein processing the client device configuration data includes determining if the client device configuration data meets predetermined security requirements.

3. (Original) The method of claim 2, wherein determining if the client device configuration data meets predetermined security requirements includes comparing the client device configuration data with reference configuration data.

4. (Previously Presented) The method of claim 2, wherein the second service access provider is further operable to update the client device configuration data if the client device configuration data fails to meet the predetermined security requirements.

-
5. (Original) The method of claim 4, wherein selectively granting the client access device access to the network includes, denying access to the network if the client device configuration data is not updated.
6. (Original) The method of claim 1, wherein the establishing of the communications link with the client access device includes, communicating an agent to the client access device, the agent operable to identify the client device configuration data and to communicate the client device configuration data to a server of the network.
7. (Original) The method of claim 6, which includes, if after the processing of the client device configuration data the client device configuration data requires an update, using the agent to update the client access device with updated configuration data.
8. (Original) The method of claim 7, which includes, after updating the client access device, receiving an update result indicator from the agent to confirm that the configuration of the client access device has been updated.
9. (Original) The method of claim 1, wherein the establishing of the communications link with the client access device includes communicating a command set, which includes at least one command, to the client access device, the command set operable to identify the client device configuration data and to communicate the client device configuration data to a server of the network.
10. (Original) The method of claim 9, which includes, if after the processing of the client device configuration data the client device configuration data requires an update, using the command set to update the client access device with updated configuration data.
11. (Original) The method of claim 10, wherein the command set further includes a first command set to identify and communicate the client device configuration data to the server, and a second command set to update the client access device with the updated configuration data.
12. (Original) The method of claim 10, which includes, after updating the client access device, receiving an update result indicator from the client access device to confirm that the configuration of the client access device has been updated.

13. (Previously Presented) The method of claim 1, the operations further including, after establishing communications with the client access device, transmitting authentication information to the second service access provider, the second service access provider further operable to authenticate the user.

14. (Original) The method of claim 13, wherein authenticating the user includes verifying user login information associated with the user attempting access to the network.

15. (Original) The method of claim 1, wherein the client device configuration data includes at least one of virus definition data, firewall configuration data, and operating system configuration data.

16. (Currently Amended) A system to verify configuration data of a client access device requesting access to a network, the system comprising:

a first service access provider, coupled to a network, to establish a communications link to the client access device to receive, from the client access device, authentication information for a user associated with the client access device and to receive the configuration data from the client access device over the communications link during an authentication and authorization exchange; and

a second service access provider to receive the authentication information and the configuration data from the first service access provider, to process the configuration data, and to selectively grant the client access device access to the network based upon the configuration data, wherein processing the configuration data includes determining if the configuration data meets predetermined security requirements.

17. (Previously Presented) The system of claim 16, wherein the second service access provider includes a configuration server to process the client device configuration data such that the configuration server determines if the client device configuration data meets predetermined security requirements.

-
18. (Original) The system of claim 17, wherein the configuration server compares the client device configuration data with reference configuration data to determine if the client device configuration data meets predetermined security requirements.
19. (Original) The system of claim 17, wherein the configuration server, after the client device configuration data is processed, updates the client device configuration data.
20. (Original) The system of claim 19, wherein the configuration server denies network access to the client access device if the client device configuration data is not updated.
21. (Previously Presented) The system of claim 17, wherein to establish the communications link with the client access device, the second service access provider communicates an agent to the client access device, the agent operable to identify the client device configuration data and to communicate the client device configuration data to at least one of the second service access provider and the configuration server.
22. (Original) The system of claim 21, wherein if after the processing of the client device configuration data the client device configuration data requires an update, the configuration server being configurable to use the agent to update client device configuration data with updated configuration data.
23. (Original) The system of claim 22, wherein after the agent updates the client access device, the configuration server receives an update result indicator from the agent to confirm that the configuration of the client device has been updated.
24. (Previously Presented) The system of claim 17, wherein to establish the communications link with the client access device, the first service access provider communicates a command set to the client access device, the command set operable to identify the client device configuration data and to communicate the client device configuration data to at least one of the first service access provider and the configuration server.
25. (Original) The system of claim 24, wherein if after the processing of the client device configuration data, the client device configuration data requires an update, the configuration server is operable to further use the command set to update client device configuration data with updated configuration data.

26. (Original) The system of claim 25, wherein after the configuration server updates the client access device, the configuration server receives an update result indicator from the client access device to confirm that the client configuration has been updated.

27. (Original) The system of claim 24, wherein the command set further includes a first command set to identify and communicate the client device configuration data to the server, and a second command set to update the client access device with the updated configuration data.

28. (Previously Presented) The system of claim 16, wherein the second service access provider includes an authentication server to authenticate and authorize a user associated with the client access device.

29. (Previously Presented) The system of claim 16, wherein the client device configuration data includes at least one of virus definition data, firewall configuration data, and operating system configuration data.

30. (Previously Presented) A machine readable medium storing a set of instructions that, when executed by a machine, cause the machine to:

perform, in a first service access provider, operations causing the machine to,

receive an access request from a client access device, the access request requesting access to a network, wherein a user associated with the client access device is a subscriber of a second service access provider;

establish a communications link with a client access device to authenticate and authorize the user associated with the client access device;

receive client device configuration data from the client access device over the communications link during an authentication and authorization exchange;

transmit the client device configuration data destined for the second service access provider, wherein the second service access provider is operable to process the client device configuration data and to selectively grant the client access device access to the network based upon the client device configuration data; and

receive an indication about whether the client access device is granted access to the network, the indication originating from the second service access provider.

31. (Original) The machine readable medium of claim 30, wherein after the processing of the client device configuration data, the client device configuration data is updated with updated configuration data.

32. (Currently Amended) A method to manage access to a network from a client access device, the method comprising:

requesting access to the network, the requesting involving a first service access provider and a second service access provider;

authenticating a user associated with the client access device in an authentication and authorization exchange, wherein the user is a subscriber of the second service access provider;

communicating client device configuration data to the second service access provider via the first service access provider;

processing the configuration data, by the second service access provider, wherein processing the configuration data includes determining if the configuration data meets predetermined security requirements;

receiving a verification response from the second service access provider via the first service access provider; and

if the user is authenticated and the verification response from the second service access provider indicates acceptance of the client device configuration data accessing the network via the first service provider.

33. (Previously Presented) The method of claim 32, wherein prior to receiving the verification response, updated configuration data is received from the second service access provider via the first service access provider, the updated configuration data to replace the client device configuration data.

34. (Currently Amended) A machine readable medium storing a set of instructions that, when executed by a machine, cause the machine to:

request, from a first service access provider, access to a network, the requesting involving a first service access provider and a second service access provider;

authenticate and authorize a user associated with the request in an authentication and authorization exchange, wherein the user is a subscriber of the second service access provider;

communicate client device configuration data the second service access provider via the first service access provider;

process the configuration data, by the second service access provider, wherein processing the configuration data includes determining if the configuration data meets predetermined security requirements;

receive a verification response from the second service access provider via the first service access provider; and

if the user is authenticated and the verification response from the second service access provider indicates acceptance of the client device configuration data, access the network via the second service provider.

35. (Previously Presented) The machine readable medium of claim 34, wherein prior to receiving a verification response, updated configuration data is received from the second service access provider to replace the client device configuration data.

36. (Canceled)